REMARKS:

Claim 36 has been cancelled and claim 35 has been amended. New claim 37 has been added. Claims 35 and 37 are pending in this application. A Request for Continued Examination (RCE) is being filed concurrently herewith.

Claims 35 and 36 were rejected under 35 U.S.C. §103(a) as being unpatentable over Fisher (U.S. Patent No. 5,005,200) in view of Payne et al. (U.S. Patent No. 5,715,314). Claim 36 has been canceled. Reconsideration with respect to claim 35 as amended and claim 37 is respectfully requested.

Applicants' invention relates to a secure user certification system for electronic commerce that provides an accounting system for services provided. In electronic commerce, various parties conduct activities without face to face contact. As such, it is desirable for each party to any transaction to be able to determine and verify the authenticity of the other party to the transaction, as well as ensure sufficient security for any commerce conducted electronically. Such security services could include, for example, message integrity, message authentication, message confidentiality, and message non-repudiation. In an electronic commerce environment these security services are achieved by cryptographic techniques such as digital signature, hash codes, encryption algorithms, and the like. To effectively implement the above, a party to an electronic commerce transaction requires access to a secure cryptographic device capable of securely implementing these cryptographic techniques. According to the present invention, a certificate meter provides certificate management services including use of cryptographically secured certificates. Payment for the processing and issuing, by the certificate authority, of the electronic certificates can be made using funds stored in the meter. Thus, the present invention provides a party to an electronic commerce transaction access to a secure cryptographic device, i.e., a certificate meter, associated with a certificate authority, while providing the certificate authority with a convenient payment system to allow the certificate authority to get paid for processing and issuing of the electronic certificates.

As illustrated in Fig. 5 of the present specification, after the certificate meter receives a request for a cryptographic certificate at 502, it is determined on 504 if sufficient funds are available in the register to obtain the certificate. If sufficient funds are available, then at 510 the certificate meter securely generates a public and private key pair. The private key is, therefore, never available outside of the secure housing of the postage and certificate meter subsystem 218. In a preferred embodiment the private key is not known to anyone, including the certificate owner, therefore the postage and certificate meter can enforce charges for any use of the private key. At step 512, the certificate meter sends a request to a certificate authority to generate a certificate including the public key of the public/private key pair generated at step 510. After the certificate has been received from the certificate authority, at step 520, funds are deducted from the register of the certificate meter for the generation of the requested certificate, which activates the user's private key. The private key can now be used to sign messages, and the signed message, along with the certificate, can be sent to a third party. The third party can use the public key contained within the certificate to verify the authenticity of the message.

In view of the above, claim 35 as amended is directed to a method for obtaining a cryptographic certificate that comprises "receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein; determining if sufficient funds are present in the register for obtaining the certificate; if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key; sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair; receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device; deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair."

Fischer, in contrast, is directed to a public key cryptographic system with enhanced digital signature certification that authenticates the identity of the public key holder. Specifically, in Fischer, a trusted authority creates a digital message which contains the claimant's public key

and the name of the claimant and a representative of the authority signs the digital message with the authority's own digital signature. This digital message, often referred to as a certificate, is sent along with the use of the claimant's own digital signature. Any recipient of the claimant's message can trust the signature, provided that the recipient recognizes the authority's public key. (Col. 3, lines 53-64). The system of Fischer provides the ability to specify a variety of attributes associated with the certification, such as specifying the authority or constraints which are conferred on the certifee by the certifier. (Col. 4, lines 56-62).

Thus, while Fischer discloses the use of certificates for providing security functions, there is no disclosure, teaching or suggestion in Fischer of "receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein, determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key" as is recited in claim 35. There is also no disclosure, teaching or suggestion in Fischer of "deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35.

The reference to Payne et al. does not overcome the above deficiencies. Payne et al. is directed to network-based sales system that includes at least one buyer computer for operation by a user desiring to buy a product, at least one merchant computer, and at least one payment computer. The computers are inter-connected by a computer network. A purchase transaction begins when a user at buyer computer 12 requests advertisements (step 24) and buyer computer 12 accordingly sends an advertising document URL (universal resource locator) to merchant computer 14 (step 26). The merchant computer fetches an advertising document from the advertising document database (step 28) and sends it to the buyer computer (step 30). The user browses through the advertising document and eventually requests a product (step 32). This results in the buyer computer sending payment URL A to the payment computer (step 34).

The payment computer sends a payment confirmation document to the buyer computer, the payment confirmation document including an "open" link and a "continue" link (step 44).

The confirmation document asks the user to click on a "continue" button if the user already has an account with the payment computer, or to click on an "open" button if the user does not already have an account and wishes to open one. If the user clicks on the "open" button (step 46), the buyer computer sends payment URL C to the payment computer (step 48), payment URL C being similar to payment URL A but also indicating that the user does not yet have an account. The payment computer creates a new account document (step 50) and sends it to the buyer computer (step 52). If the user clicks on the "continue" button (step 60), the buyer computer sends payment URL B to the payment computer (step 62), payment URL B being similar to payment URL A but also indicating that the user already has an account. The payment computer then instructs the buyer computer to provide the account name and password (steps 64 and 66), and the buyer computer prompts the user for this information by creating an account name prompt (example shown in FIG. 8) and a similar password prompt. The user enters the information (step 68) and the buyer computer sends the account name and password to the payment computer (step 70). The payment computer checks the settlement database to determine whether the user has unexpired access to the domain identifier contained in the payment URL (step 82). If so, the payment computer sends to the buyer computer a document providing an option either to repurchase or to use the previously purchased access (step 84). The user can respond to the recent purchase query document by choosing to access the previously purchased document (step 85) or to go ahead and buy the currently selected product (step 86). If the user chooses to buy the currently selected product, the payment computer calculates an actual payment amount that may differ from the payment amount contained in the payment URL (step 87). For example, the purchase of a product in a certain domain may entitle the user to access other products in the domain for free or for a reduced price for a given period of time. The payment computer then verifies whether the user account has sufficient funds or credit (step 76). If not, the payment computer sends a document to the buyer computer indicating that the user account has insufficient funds (step 78). (Col. 5, line 16 to Col. 7, line 20).

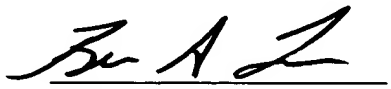
Thus, if Payne et al. teaches anything at all, it is merely a conventional network based sales system that utilizes a credit card account to pay for purchases made on-line. There is no disclosure, teaching or suggestion in Payne of any type of a "metering device including a register

having funds stored therein" as is recited in claim 35. There is also no disclosure, teaching or suggestion in Payne et al. of "receiving at a metering device a request for a cryptographic certificate . . . determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key; sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair; receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device; deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35.

For at least the above reasons, Applicants respectfully submit that claim 35 as amended is allowable over the prior art of record. Claim 37, dependent upon claim 35, is allowable along with claim 35 and on its own merits.

In view of the foregoing amendments and remarks, it is respectfully submitted that the pending claims are in a condition for allowance and favorable action thereon is requested.

Respectfully submitted,



Brian A. Lemm
Reg. No. 43,748
Attorney for Applicants
Telephone No.: (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000